The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Acrobat 9 uses more efficient encryption than previous versions, which makes it easier for attackers to guess a document's password via a brute-force attack.	2008-12-04	7.5	CVE-2008-5331 BID MISC CONFIRM
apple -- cups	Integer overflow in the _cupsImageReadPNG function in CUPS 1.1.17 through 1.3.9 allows remote attackers to execute arbitrary code via a PNG image with a large height value, which bypasses a validation check and triggers a buffer overflow.	2008-12-01	7.5	CVE-2008-5286 BID CONFIRM
apple -- iphone_configuration_web_utility	Directory traversal vulnerability in the web interface in Apple iPhone Configuration Web Utility 1.0 on Windows allows remote attackers to read arbitrary files via unspecified vectors.	2008-12-03	7.8	CVE-2008-5315 BUGTRAQ SECUNIA FULLDISC
bdigital_web_solutions -- webstudio_ehotel	SQL injection vulnerability in index.php in WebStudio eHotel allows remote attackers to execute arbitrary SQL commands via the pageid parameter.	2008-12-01	7.5	CVE-2008-5293 XF MILW0RM SECUNIA
bdigital_web_solutions -- webstudio_ecatalogue	SQL injection vulnerability in index.php in WebStudio eCatalogue allows remote attackers to execute arbitrary SQL commands via the pageid parameter.	2008-12-01	7.5	CVE-2008-5294 XF MILW0RM SECUNIA
bdigital_web_solutions -- webstudio_cms	SQL injection vulnerability in index.php in WebStudio CMS allows remote attackers to execute arbitrary SQL commands via the pageid parameter.	2008-12-04	7.5	CVE-2008-5336 BID BUGTRAQ MILW0RM
easy-script -- wysi_wiki_wyg	Wysi Wiki Wyg 1.0 allows remote attackers to obtain system information via an invalid categup parameter to index.php, which calls the phpinfo function.	2008-12-03	7.8	CVE-2008-5322 MILW0RM SECUNIA MISC

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fuzzylime -- fuzzylime_cms	Directory traversal vulnerability in code/track.php in FuzzyLime 3.03 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the p parameter, a different vector than CVE-2007-4805 and CVE-2008-3165.	2008-12-01	7.5	CVE-2008-5291 BID MILW0RM SECUNIA
ibm -- rational_clearquest	ClearQuest Web in IBM Rational ClearQuest MultiSite before 7.1 allows remote servers to direct a client's submissions and changes to an arbitrary database by specifying multiple comma-separated server identifiers on the JTLRMIREGISTRYSERVERS line in a jtl.properties file.	2008-12-04	7.5	CVE-2008-5329 XF AIXAPAR SECUNIA
iea_software -- air_marshal iea_software -- emerald iea_software -- radius_test_client iea_software -- radiusnt iea_software -- radiusx iea_software -- radlogin	The web server in IEA Software RadiusNT and RadiusX 5.1.38 and other versions before 5.1.44, Emerald 5.0.49 and other versions before 5.0.52, Air Marshal 2.0.4 and other versions before 2.0.8, and Radius test client (aka Radlogin) 4.0.20 and earlier, allows remote attackers to cause a denial of service (crash) via an HTTP Content-Length header with a negative value, which triggers a single byte overwrite of memory using a NULL terminator. NOTE: some of these details are obtained from third party information.	2008-11-28	10.0	CVE-2008-5284 BID CONFIRM CONFIRM CONFIRM FRSIRT SECUNIA MISC
inspector_it -- wiz-ad	SQL injection vulnerability in Wiz-Ad 1.3 allows remote attackers to execute arbitrary SQL commands via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-12-04	7.5	CVE-2007-6719 BID
jamit_software -- jamit_job_board	SQL injection vulnerability in index.php in Jamit Job Board 3.4.10 allows remote attackers to execute arbitrary SQL commands via the show_emp parameter.	2008-12-01	7.5	CVE-2008-5295 BID MILW0RM SECUNIA
littlecms -- lcms littlecms -- little_cms_color_engine	Buffer overflow in the ReadEmbeddedTextTag function in src/cmsio1.c in Little cms color engine (aka lcms) before 1.16 allows attackers to have an unknown impact via vectors related to a length parameter inconsistency involving the contents of "the input file," a different vulnerability than CVE-2007-2741.	2008-12-03	10.0	CVE-2008-5316 CONFIRM
littlecms -- lcms littlecms -- little_cms_color_engine	Integer signedness error in the cmsAllocGamma function in src/cmsgamma.c in Little cms color engine (aka lcms) before 1.17 allows attackers to have an unknown impact via a file containing a certain "number of entries" value, which is interpreted improperly, leading to an allocation of insufficient memory.	2008-12-03	10.0	CVE-2008-5317 CONFIRM
lovecms -- the_simple_forum	The Simple Forum 3.1d module for LoveCMS 1.6.2 Final does properly restrict access to administrator functions, which allows remote attackers to change the administrator password via a direct request to modules/simpleforum/admin/index.php.	2008-12-02	7.5	CVE-2008-5308 XF BID MILW0RM FRSIRT SECUNIA

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				OSVDB
multimania -- bandsite_portal_system multimania -- bandwebsite	SQL injection vulnerability in lyrics.php in Bandwebsite (aka Bandsite portal system) 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-04	7.5	CVE-2008-5337 MISC BID MILW0RM
netart_media -- real_estate_portal	SQL injection vulnerability in NetArt Media Real Estate Portal 1.2 allows remote attackers to execute arbitrary SQL commands via the ad_id parameter in the re_send_email module to index.php.	2008-12-02	7.5	CVE-2008-5309 XF BID MILW0RM
netart_media -- car_portal	SQL injection vulnerability in image.php in NetArt Media Car Portal 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-02	7.5	CVE-2008-5310 XF BID MILW0RM FRSIRT
netart_media -- blog_system	SQL injection vulnerability in image.php in NetArt Media Blog System 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-02	7.5	CVE-2008-5311 XF BID MILW0RM FRSIRT
nitrotech -- nitrotech	SQL injection vulnerability in members.php in NitroTech 0.0.3a allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-04	7.5	CVE-2008-5333 BID MILW0RM
nitrotech -- nitrotech	PHP remote file inclusion vulnerability in includes/common.php in NitroTech 0.0.3a allows remote attackers to execute arbitrary PHP code via a URL in the root parameter.	2008-12-04	10.0	CVE-2008-5334 MILW0RM
octeth -- oempro	Multiple SQL injection vulnerabilities in Octeth Oempro 3.5.5.1, and possibly other versions before 4, allow remote attackers to execute arbitrary SQL commands via the FormValue_Email parameter (aka Email field) to index.php in (1) member/, (2) client/, or (3) admin/; or (4) the FormValue_SearchKeywords parameter to client/campaign_track.php.	2008-12-03	7.5	CVE-2008-3058 OSVDB OSVDB MISC MISC
pie -- pie	Multiple PHP remote file inclusion vulnerabilities in Pie 0.5.3 allow remote attackers to execute arbitrary PHP code via a URL in the (1) lib parameter to files in lib/action/ including (a) alias.php, (b) cancel.php, (c) context.php, (d) deadlinks.php, (e) delete.php, and others; and the (2) GLOBALS[pie][library_path] parameter to files in lib/share/ including (f) diff.php, (g) file.php, (h) locale.php, (i) mapfile.php, (j) page.php, and others.	2008-12-04	10.0	CVE-2008-5332 BID MILW0RM
pilot_group -- pg_real_estate_solution	SQL injection vulnerability in admin/index.php in PG Real Estate Solution allows remote attackers to execute arbitrary SQL commands via the login_lg parameter (username). NOTE: some of these details are obtained from third party information.	2008-12-02	7.5	CVE-2008-5306 XF BID MILW0RM FRSIRT SECUNIA

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pilot_group -- pg_real_roommate_finder_solution	SQL injection vulnerability in admin/index.php in PG Roommate Finder Solution allows remote attackers to execute arbitrary SQL commands via the login_lg parameter. NOTE: some of these details are obtained from third party information.	2008-12-02	7.5	CVE-2008-5307 XF BID MILW0RM FRSIRT SECUNIA
samba -- samba	smbd in Samba 3.0.29 through 3.2.4 might allow remote attackers to read arbitrary memory and cause a denial of service via crafted (1) trans, (2) trans2, and (3) nttrans requests, related to a "cut&paste error" that causes an improper bounds check to be performed.	2008-12-01	8.5	CVE-2008-4314 UBUNTU SECTRACK BID FRSIRT CONFIRM CONFIRM SECUNIA SECUNIA OSVDB
scripts4you -- faq_manager	SQL injection vulnerability in catagorie.php in Werner Hilversum FAQ Manager 1.2 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2008-12-01	7.5	CVE-2008-5287 XF BID MILW0RM SECUNIA
scripts4you -- clean_cms	SQL injection vulnerability in full_txt.php in Werner Hilversum Clean CMS 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-12-01	7.5	CVE-2008-5289 BID MILW0RM MILW0RM SECUNIA
sun -- jdk sun -- jre sun -- sdk	Sun Java Web Start and Java Plug-in for JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allow remote attackers to execute arbitrary code via a crafted jnlp file that modifies the (1) java.home, (2) java.ext.dirs, or (3) user.home System Properties, aka "Java Web Start File Inclusion."	2008-12-04	9.3	CVE-2008-2086 MISC BUGTRAQ REDHAT SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows untrusted JWS applications to gain privileges to access local files or applications via unknown vectors.	2008-12-05	10.0	CVE-2008-5340 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows "hidden code" to make unauthorized network connections and "hijack HTTP sessions using cookies stored in the browser" via unknown vectors.	2008-12-05	9.0	CVE-2008-5343 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows	2008-12-05	7.5	CVE-2008-5344 SUNALERT

Back to top

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	untrusted applets to read arbitrary files and make unauthorized network connections via unknown vectors related to applet classloading.			
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Runtime Environment (JRE) with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 and earlier allows code that is loaded from a local filesystem to read arbitrary files and make unauthorized connections to localhost via unknown vectors.	2008-12-05	7.5	CVE-2008-5345 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Runtime Environment (JRE) for Sun JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 or earlier allows untrusted applets and applications to read arbitrary memory via a crafted ZIP file.	2008-12-05	7.1	CVE-2008-5346 SUNALERT
sun -- jdk sun -- jre	Multiple unspecified vulnerabilities in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier allow untrusted applets and applications to gain privileges via vectors related to access to inner classes in the (1) JAX-WS and (2) JAXB packages.	2008-12-05	7.5	CVE-2008-5347 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier, when using Kerberos authentication, allows remote attackers to cause a denial of service (OS resource consumption) via unknown vectors.	2008-12-05	7.1	CVE-2008-5348 SUNALERT
sun -- jdk sun -- jre	Unspecified vulnerability in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier, and JDK and JRE 5.0 Update 16 and earlier, allows remote attackers to cause a denial of service (CPU consumption) via a crafted RSA public key.	2008-12-05	7.1	CVE-2008-5349 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier accepts UTF-8 encodings that are not the "shortest" form, which makes it easier for attackers to bypass protection mechanisms for other applications that rely on shortest-form UTF-8 encodings.	2008-12-05	7.5	CVE-2008-5351 SUNALERT
sun -- jdk sun -- jre	Integer overflow in the JAR unpacking utility (unpack200) in the unpack library (unpack.dll) in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier, and JDK and JRE 5.0 Update 16 and earlier, allows untrusted applications and applets to gain privileges via a Pack200 compressed JAR file that triggers a heap-based buffer overflow.	2008-12-05	9.3	CVE-2008-5352 SUNALERT

Back to top

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows untrusted applets and applications to gain privileges via unknown vectors related to "deserializing calendar objects."	2008-12-05	10.0	CVE-2008-5353 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Stack-based buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows locally-launched and possibly remote untrusted Java applications to execute arbitrary code via a JAR file with a long Main-Class manifest entry.	2008-12-05	9.3	CVE-2008-5354 SUNALERT
sun -- jdk sun -- jre sun -- sdk	The "Java Update" feature for Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier does not verify the signature of the JRE that is downloaded, which allows remote attackers to execute arbitrary code via DNS man-in-the-middle attacks.	2008-12-05	10.0	CVE-2008-5355 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Heap-based buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier might allow remote attackers to execute arbitrary code via a crafted TrueType font file.	2008-12-05	9.3	CVE-2008-5356 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Integer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 and earlier might allow remote attackers to execute arbitrary code via a crafted TrueType font file, which triggers a heap-based buffer overflow.	2008-12-05	9.3	CVE-2008-5357 IDEFENSE
sun -- jdk sun -- jre	Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier might allow remote attackers to execute arbitrary code via a crafted GIF file that triggers memory corruption during display of the splash screen, possibly related to splashscreen.dll.	2008-12-05	9.3	CVE-2008-5358 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 and earlier might allow remote attackers to execute arbitrary code via unknown vectors related to "image processing code."	2008-12-05	9.3	CVE-2008-5359 SUNALERT
videogirls -- videogirls_biz	SQL injection vulnerability in view_snaps.php in VideoGirls BiZ, allows remote attackers to execute arbitrary SQL commands via the type parameter.	2008-12-01	7.5	CVE-2008-5292 BID MILW0RM

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				SECUNIA
videolan -- vlc_media_player	Integer overflow in the ReadRealIndex function in real.c in the Real demuxer plugin in VideoLAN VLC media player 0.9.0 through 0.9.7 allows remote attackers to execute arbitrary code via a malformed RealMedia (.rm) file that triggers a heap-based buffer overflow.	2008-12-03	9.3	CVE-2008-5276 CONFIRM MISC BID BUGTRAQ OSVDB FRSIRT SECUNIA CONFIRM
vitalwerks -- no-ip_duc	Buffer overflow in No-IP DUC 2.1.7 and earlier allows remote DNS servers to execute arbitrary code via a crafted DNS response, related to a missing length check in the GetNextLine function.	2008-12-01	7.6	CVE-2008-5297 MISC MLIST MILW0RM CONFIRM CONFIRM
xoops_hocasi -- gesgaleri	SQL injection vulnerability in index.php in GesGaleri, a module for XOOPS, allows remote attackers to execute arbitrary SQL commands via the no parameter.	2008-12-03	7.5	CVE-2008-5321 XF BID MILW0RM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Multiple cross-site scripting (XSS) vulnerabilities in CQ Web in IBM Rational ClearQuest 2007 before 2007D and 2008 before 2008B allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-12-04	4.3	CVE-2008-5324 AIXAPAR
awstats -- awstats	awstats.pl in AWStats 6.8 and earlier does not properly remove quote characters, which allows remote attackers to conduct cross-site scripting (XSS) attacks via the query_string parameter. NOTE: this issue exists because of an incomplete fix for CVE-2008-3714.	2008-12-03	4.3	CVE-2008-5080 CONFIRM MISC
clam_anti-virus -- clamav	Stack consumption vulnerability in libclamav/special.c in ClamAV before 0.94.2 allows remote attackers to cause a denial of service (daemon crash) via a crafted JPEG file, related to the cli_check_jpeg_exploit, jpeg_check_photoshop, and jpeg_check_photoshop_8bim functions.	2008-12-03	4.3	CVE-2008-5314 CONFIRM MLIST MLIST
debian -- mailscanner	mailscanner 4.55.10 might allow local users to overwrite arbitrary files via a symlink attack on certain temporary files used by the (1) f-prot-autoupdate, (2) clamav-autoupdate, (3) panda-autoupdate.new, (4)	2008-12-03	6.9	CVE-2008-5312 MLIST MISC

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	trend-autoupdate.new, and (5) rav-autoupdate.new scripts in /etc/MailScanner/autoupdate/, a different vulnerability than CVE-2008-5140.			
debian -- mailscanner	mailscanner 4.68.8 might allow local users to overwrite arbitrary files via a symlink attack on certain temporary files used by the (1) f-prot-autoupdate, (2) clamav-autoupdate, (3) avast-autoupdate, and (4) f-prot-6-autoupdate scripts in /etc/MailScanner/autoupdate/; the (5) bitdefender-wrapper, (6) kaspersky-wrapper, (7) clamav-wrapper, and (8) rav-wrapper scripts in /etc/MailScanner/wrapper/; the (9) Quarantine.pm, (10) TNEF.pm, (11) MessageBatch.pm, (12) WorkArea.pm, and (13) SA.pm scripts in /usr/share/MailScanner/MailScanner/; (14) /usr/sbin/MailScanner; and (15) scripts that load the /etc/MailScanner/mailscanner.conf.with.mcp configuration file.	2008-12-03	6.9	CVE-2008-5313 MLIST MISC
dovecot -- dovecot	Directory traversal vulnerability in the ManageSieve implementation in Dovecot 1.0.15, 1.1, and 1.2 allows remote attackers to read and modify arbitrary .sieve files via a ".." (dot dot) in a script name.	2008-12-01	6.4	CVE-2008-5301 MLIST
e107 -- e107	SQL injection vulnerability in usersettings.php in e107 0.7.13 and earlier allows remote authenticated users to execute arbitrary SQL commands via the ue[] parameter.	2008-12-03	6.5	CVE-2008-5320 XF BID MILW0RM FRSIRT SECUNIA
easy-script -- wysi_wiki_wyg	Cross-site scripting (XSS) vulnerability in index.php in Wysi Wiki Wyg 1.0 allows remote attackers to inject arbitrary web script or HTML via the s parameter.	2008-12-03	4.3	CVE-2008-5323 XF BID MILW0RM SECUNIA MISC
experts -- experts	SQL injection vulnerability in answer.php in Experts 1.0.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the question_id parameter.	2008-11-28	6.8	CVE-2008-5267 XF BID MILW0RM
gallery -- gallery	Gallery 1.5.x before 1.5.10 and 1.6 before 1.6-RC3, when register_globals is enabled, allows remote attackers to bypass authentication and gain administrative via unspecified cookies. NOTE: some of these details are obtained from third party information.	2008-12-01	6.8	CVE-2008-5296 CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ghh -- google_hack_honeypot_file_upload_manager	Google Hack Honeypot (GHH) File Upload Manager 1.3 allows remote attackers to delete uploaded files via unknown vectors related to the delall action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. CVE analysis suggests that the most recent version as of 20081128 is 1.2, and the File Upload Manager does not have a "delall" action.	2008-11-28	6.4	CVE-2008-5283 BID
hp -- hp-ux	Unspecified vulnerability in the kernel in HP HP-UX B.11.31 allows local users to cause a denial of service via unknown vectors.	2008-12-04	4.6	CVE-2008-4416 XF BID SECTRACK SECUNIA HP
ibm -- rational_clearquest	Multiple cross-site scripting (XSS) vulnerabilities in CQ Web in IBM Rational ClearQuest 7.0.0 before 7.0.0.4 and 7.0.1 before 7.0.1.3 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-12-04	4.3	CVE-2008-5325 BID OSVDB AIXAPAR SECUNIA
ibm -- rational_clearquest	The ClearQuest Maintenance Tool in IBM Rational ClearQuest 7.0.0 before 7.0.0.4 and 7.0.1 before 7.0.1.3 on Windows allows local users to obtain (1) user and (2) database passwords by using a password revealer utility on a field containing a series of asterisks.	2008-12-04	4.4	CVE-2008-5326 XF BID AIXAPAR SECUNIA
ibm -- rational_clearquest	The ClearQuest Maintenance Tool in IBM Rational ClearQuest 7 before 7.1 stores the database password in cleartext in an object in a ClearQuest connection profile or export file, which allows remote authenticated users to obtain sensitive information by locating the password object within the object tree.	2008-12-04	6.5	CVE-2008-5327 XF AIXAPAR SECUNIA
ibm -- rational_clearquest	The ClearQuest Maintenance Tool in IBM Rational ClearQuest before 7 stores the database password in cleartext in an object in a ClearQuest connection profile or export file, which allows remote authenticated users to obtain sensitive information by locating the password object within the object tree during an import process.	2008-12-04	4.6	CVE-2008-5328 XF AIXAPAR SECUNIA
ibm -- rational_clearquest	Multiple cross-site scripting (XSS) vulnerabilities in the web interface in ClearCase RWP server in IBM Rational ClearCase 7.0.0 before 7.0.0.4, and 7.0.1.1-RATL-RCC-IFIX02 and possibly other 7.0.1 versions before 7.0.1.3, allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO of a	2008-12-04	4.3	CVE-2008-5330 BID AIXAPAR SECTRACK SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	URI associated with a VOB page.			
karakas-online -- chm2pdf	chm2pdf 0.9 allows user-assisted local users to delete arbitrary files via a symlink attack on .chm files in the (1) /tmp/chm2pdf/work or (2) /tmp/chm2pdf/orig temporary directories.	2008-12-01	6.9	CVE-2008-5299 CONFIRM
linux -- kernel	Linux kernel 2.6.28 allows local users to cause a denial of service ("soft lockup" and process loss) via a large number of sendmsg function calls, which does not block during AF_UNIX garbage collection and triggers an OOM condition, a different vulnerability than CVE-2008-5029.	2008-12-01	4.9	CVE-2008-5300 CONFIRM MLIST MLIST
multimania -- bandsite_portal_system multimania -- bandwebsite	Cross-site scripting (XSS) vulnerability in info.php in Bandwebsite (aka Bandsite portal system) 1.5 allows remote attackers to inject arbitrary web script or HTML via the section parameter.	2008-12-04	4.3	CVE-2008-5338 MISC BID MILW0RM
octeth -- oempro	Octeth Oempro 3.5.5.1, and possibly other versions before 4, does not set the secure flag for the PHPSESSID cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2008-12-03	5.0	CVE-2008-3057 OSVDB MISC MISC
octeth -- oempro	member/settings_account.php in Octeth Oempro 3.5.5.1, and possibly other versions before 4, uses cleartext to transmit a password entered in the FormValue_Password field, which makes it easier for remote attackers to obtain sensitive information by sniffing the network, related to the "Settings - Account Information" tab.	2008-12-03	4.0	CVE-2008-3059 OSVDB MISC MISC
perl -- file::path	Race condition in the rmtree function in File::Path 1.08 and 2.07 (lib/File/Path.pm) in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is different from CVE-2008-5303 due to affected versions.	2008-12-01	6.9	CVE-2008-5302 MLIST MISC CONFIRM CONFIRM
perl -- file::path	Race condition in the rmtree function in File::Path 1.08 (lib/File/Path.pm) in Perl 5.8.8 allows local users to allows local users to delete arbitrary files via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is	2008-12-01	6.9	CVE-2008-5303 MLIST MISC CONFIRM CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	different from CVE-2008-5302 due to affected versions.			
php-fusion -- php-fusion	SQL injection vulnerability in messages.php in PHP-Fusion 6.01.15 and 7.00.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the subject and msg_send parameters, a different vector than CVE-2005-3157, CVE-2005-3158, CVE-2005-3159, CVE-2005-4005, and CVE-2006-2459.	2008-12-04	6.8	CVE-2008-5335 CONFIRM CONFIRM CONFIRM
scripts4you -- faq_manager	PHP remote file inclusion vulnerability in include/header.php in Werner Hilversum FAQ Manager 1.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the config_path parameter.	2008-12-01	6.8	CVE-2008-5288 BID MILW0RM SECUNIA
scripts4you -- clean_cms	Cross-site scripting (XSS) vulnerability in full_txt.php in Werner Hilversum Clean CMS 1.5 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2008-12-01	4.3	CVE-2008-5290 BID MILW0RM SECUNIA
squirrelmail -- squirrelmail	Cross-site scripting (XSS) vulnerability in SquirrelMail before 1.4.17 allows remote attackers to inject arbitrary web script or HTML via a crafted hyperlink in an HTML part of an e-mail message.	2008-12-04	6.8	CVE-2008-2379 XF CONFIRM BID MISC SECUNIA
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows untrusted JWS applications to perform network connections to unauthorized hosts via unknown vectors.	2008-12-05	5.0	CVE-2008-5339 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier, and JDK and JRE 5.0 Update 16 and earlier, allows untrusted JWS applications to obtain the pathname of the JWS cache and the application username via unknown vectors.	2008-12-05	5.0	CVE-2008-5341 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in the BasicService for Java Web Start (JWS) and Java Plug-in with Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows untrusted downloaded applications to cause local files to be displayed in the browser of the user of the untrusted application via unknown vectors.	2008-12-05	5.0	CVE-2008-5342 SUNALERT

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier allows untrusted applications and applets to list the contents of the operating user's directory via unknown vectors.	2008-12-05	5.0	CVE-2008-5350 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 and earlier creates temporary files with predictable file names, which allows attackers to write malicious JAR files via unknown vectors.	2008-12-05	6.4	CVE-2008-5360 SUNALERT
tikiwiki -- tikiwiki	Unspecified vulnerability in Tikiwiki before 2.2 has unknown impact and attack vectors related to "size of user-provided input," a different issue than CVE-2008-3653.	2008-12-03	5.0	CVE-2008-5318 CONFIRM
tikiwiki -- tikiwiki	Unspecified vulnerability in Tikiwiki before 2.2 has unknown impact and attack vectors related to tiki-error.php, a different issue than CVE-2008-3653.	2008-12-03	5.0	CVE-2008-5319 OSVDB CONFIRM SECUNIA CONFIRM
tntforum -- tnt_forum	Directory traversal vulnerability in index.php in TNT Forum 0.9.4, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the modulo parameter.	2008-11-28	6.8	CVE-2008-5265 BID MILW0RM SECUNIA
wireshark -- wireshark	Wireshark 1.0.4 and earlier allows remote attackers to cause a denial of service via a long SMTP request, which triggers an infinite loop.	2008-12-01	5.0	CVE-2008-5285 SECUNIA
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in the self_link function in in the RSS Feed Generator (wp-includes/feed.php) for WordPress before 2.6.5 allows remote attackers to inject arbitrary web script or HTML via the Host header (HTTP_HOST variable).	2008-11-28	4.3	CVE-2008-5278 CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
karakas-online -- chm2pdf	chm2pdf 0.9 uses temporary files in directories with fixed names, which allows local users to cause a denial of service (chm2pdf failure) of other users by creating those	2008-12-01	2.1	CVE-2008-5298 CONFIRM

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	directories ahead of time.			

Back to top